КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

# ПРЕЗЕНТАЦІЯ

ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ МАГІСТРА

на тему: «Технологія інтелектуального захисту інформації критично важливих об'єктів»

Виконав студент 2-го курсу, групи БІКСм-24
Андрєєв Марк Анатолійович.
Науковий керівник:
к.т.н.., доцент Шабала Є.Є.

.

**Актуальність проблеми:** У зв'язку зі зростанням складності та різноманітності кіберзагроз, а також з урахуванням обмежень традиційних методів діагностики, актуалізується необхідність розробки ефективних підходів до захисту критично важливих об'єктів в умовах розподілених систем.

**Метою дослідження** є розробка технології інтелектуального захисту, що забезпечує комплексну діагностику, своєчасне виявлення аномалій та підвищення надійності критично важливих об'єктів на основі аналізу мережевого трафіку. Для досягнення поставленої мети визначено наступні завдання:

- Розробка підходу до комплексної діагностики.
- Виявлення мережевих аномалій для своєчасної ідентифікації загроз.
- Підвищення рівня надійності, стабільності та безпеки критичної інфраструктури.

**Наукова новизна** полягає в інтеграції концепцій та технологій, таких як штучний інтелект, машинне навчання та аналіз великих даних, в єдину систему інтелектуального захисту критично важливих об'єктів.

**Предметом дослідження** є методи та засоби діагностики мережевих аномалій на основі аналізу мережевого трафіку, застосовані для інтелектуального захисту критично важливих об'єктів.

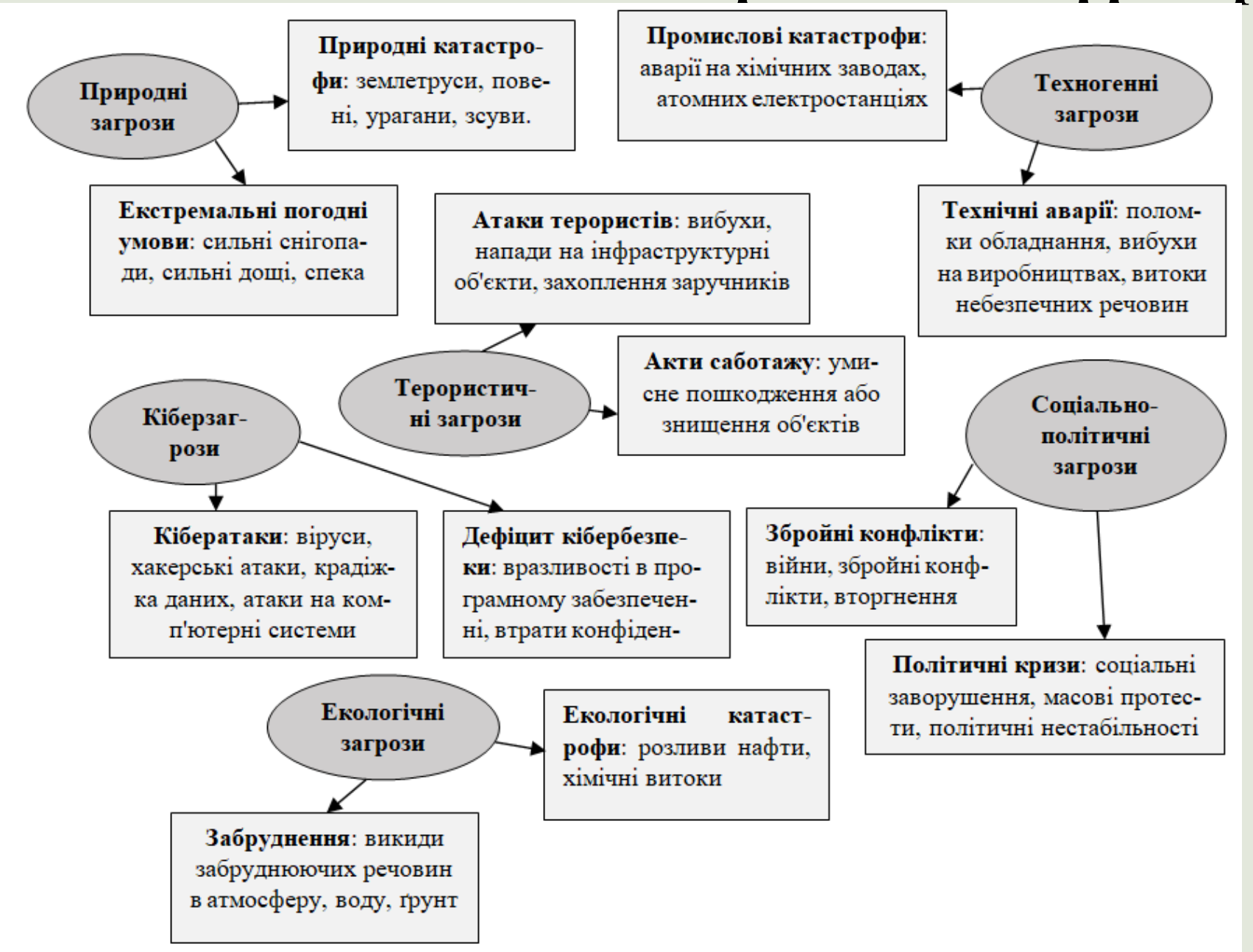
**Об'єктом дослідження** є комп'ютерна мережа з багаторівневою системою безпеки, що імітує структуру критично важливого об'єкта і потребує ефективних методів захисту від кіберзагроз.

# Задачі

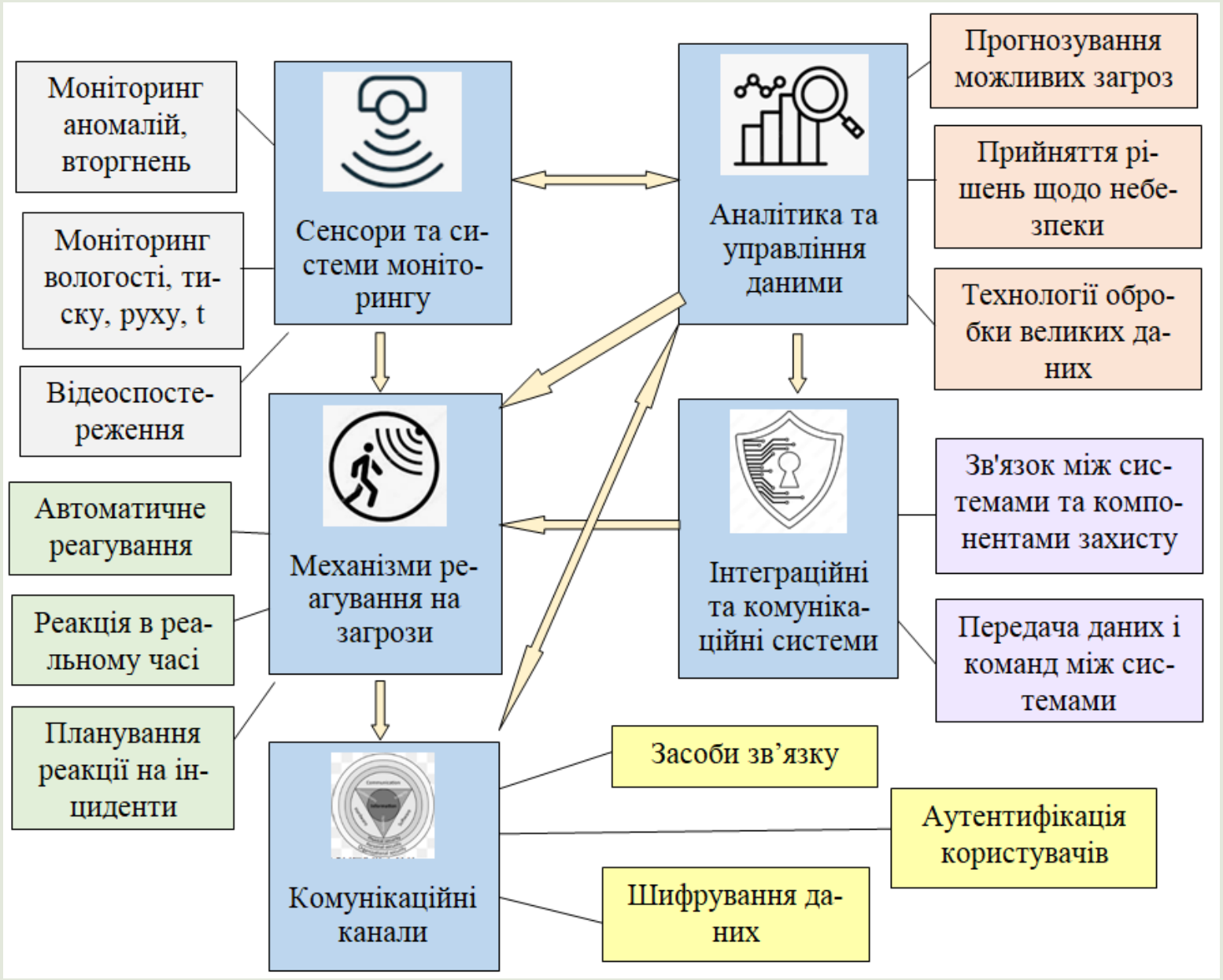
1. Провести аналіз загроз кібербезпеці критичної інфраструктури та сучасних стандартів захисту критично важливих об’єктів (КВО).
2. Дослідити сучасні підходи до моніторингу та аналізу мережевого трафіку.
3. Розглянути методи виявлення та прогнозування мережевих аномалій.
4. Проаналізувати алгоритми машинного навчання та глибокого навчання, які можуть бути застосовані для інтелектуального захисту КВО.
5. Розробити структурну та функціональну моделі технології інтелектуального захисту інформації КВО.
6. Розробити та обґрунтувати архітектуру системи захисту КВО на основі машинного навчання та систем фізичного захисту

# Класифікація об’єктів критичної інфраструктури

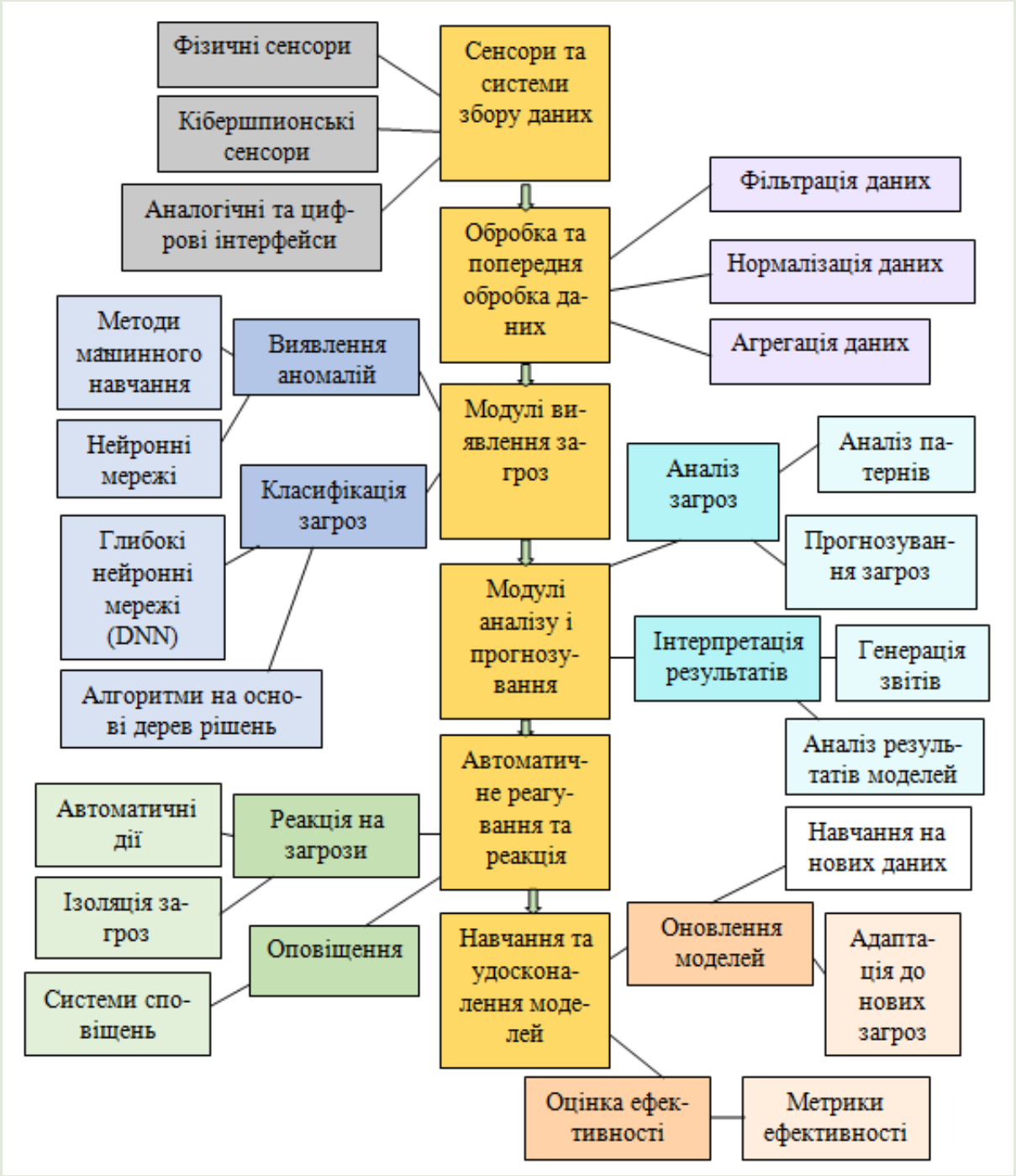

# Потенційні впливи на об'єкти критичної інфраструктури



# Схема архітектури системи інтелектуального захисту критично важливих об'єктів

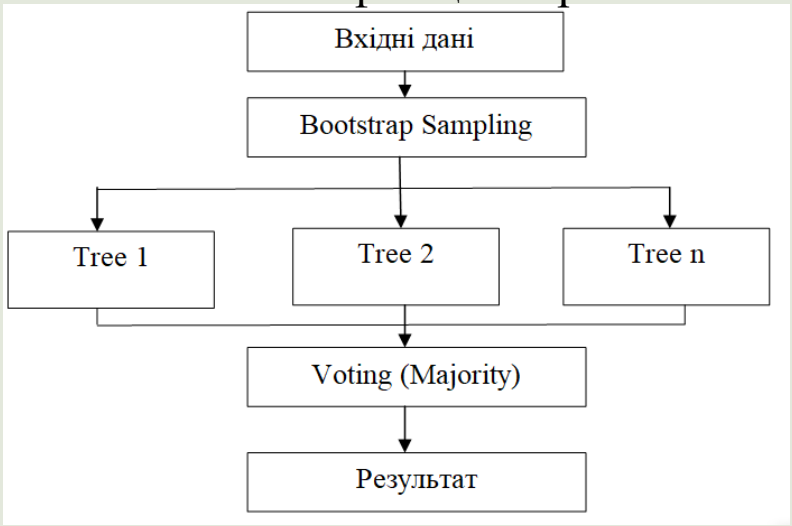


# Архітектура системи штучного інтелекту для захисту критично важливих об’єктів



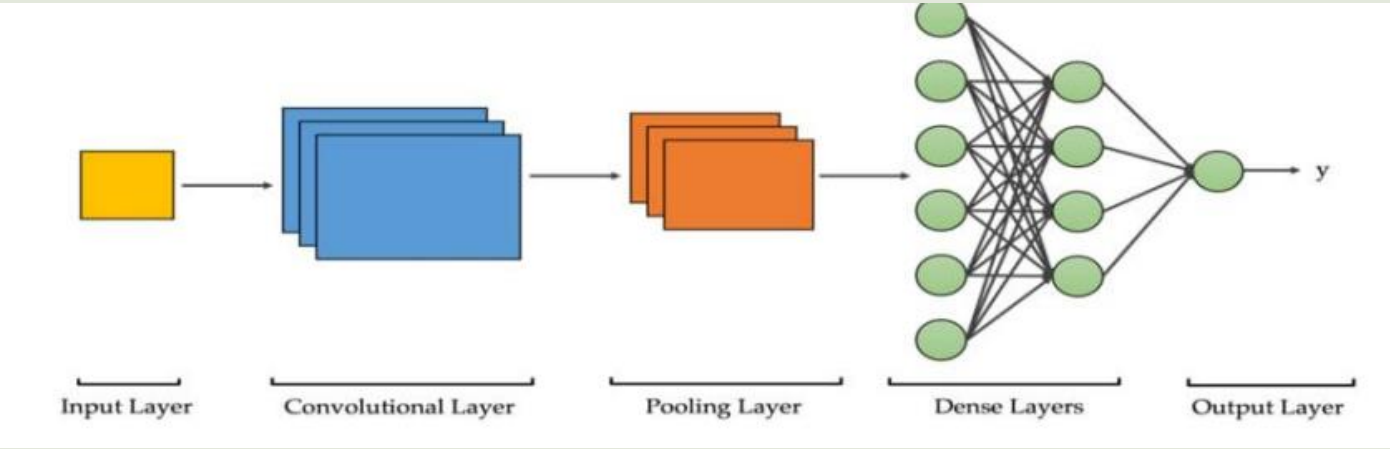
# Модулі виявлення загроз

Схема алгоритму Random Forest для класифікації загроз




Алгоритм застосування K-means для захисту критичної інфраструктури

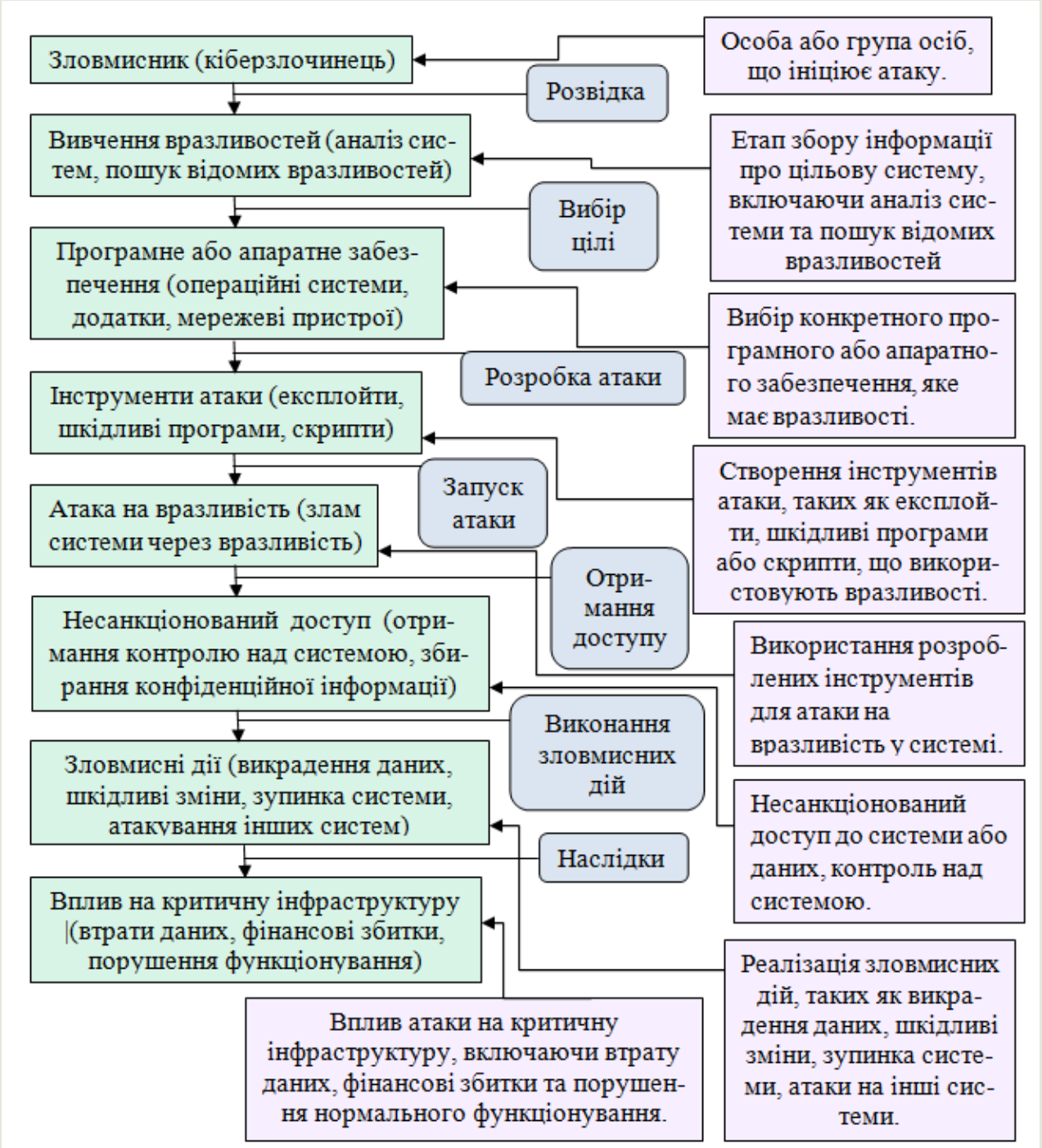

Схема архітектури згорткової мережі



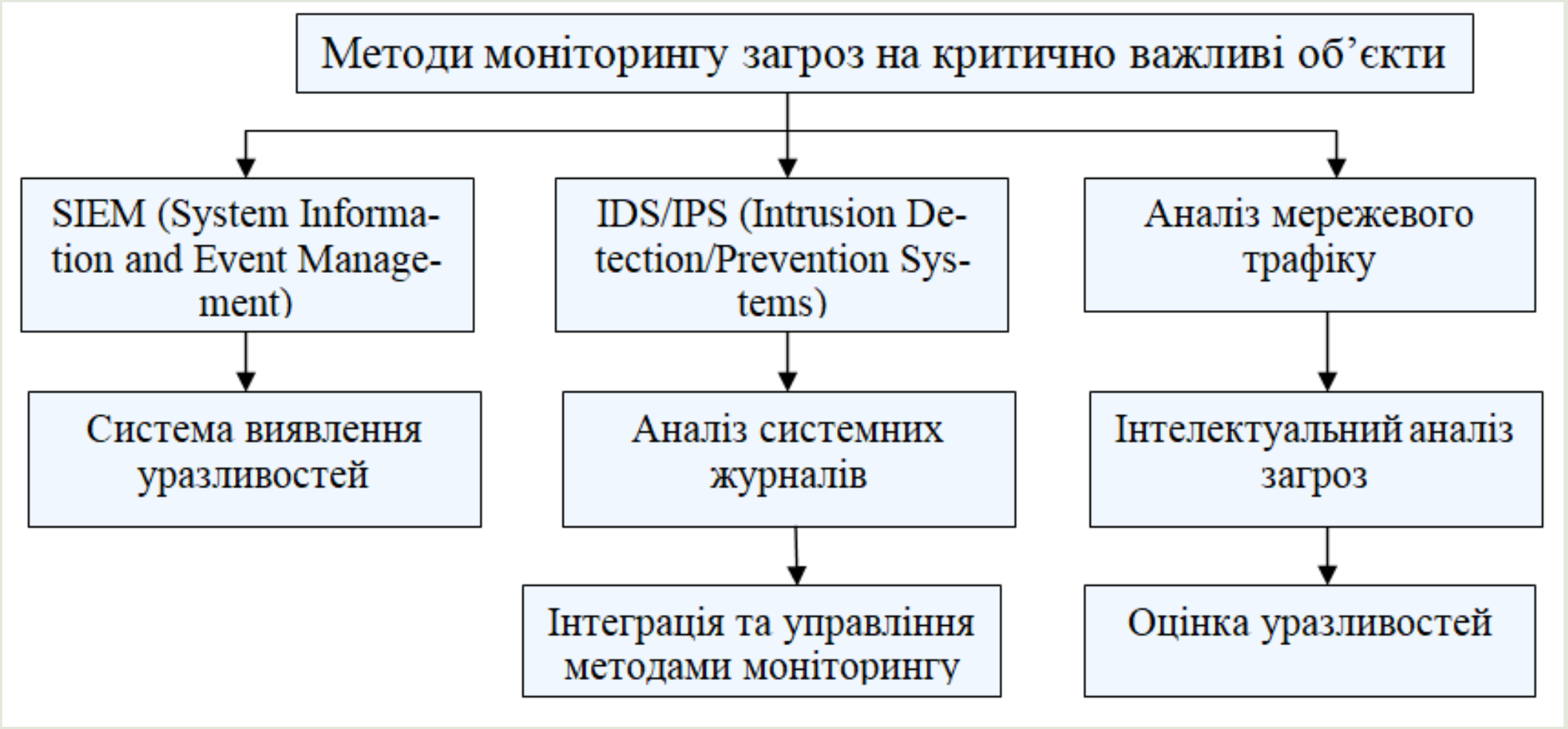
# Застосування IoT в системах інтелектуального захисту критично важливих об’єктах

# Модель DDoS атаки на критичну інфраструктуру

# Модель атак, спрямовані на використання вразливостей програмного чи апаратного забезпечення на критичну інфраструктуру



# Методи моніторингу загроз на критично важливі об’єкти



# Алгоритм реагування на інциденти загроз на критичну інфраструктуру

# Завдання системи відеоспостереження для критично важливих об’єктів

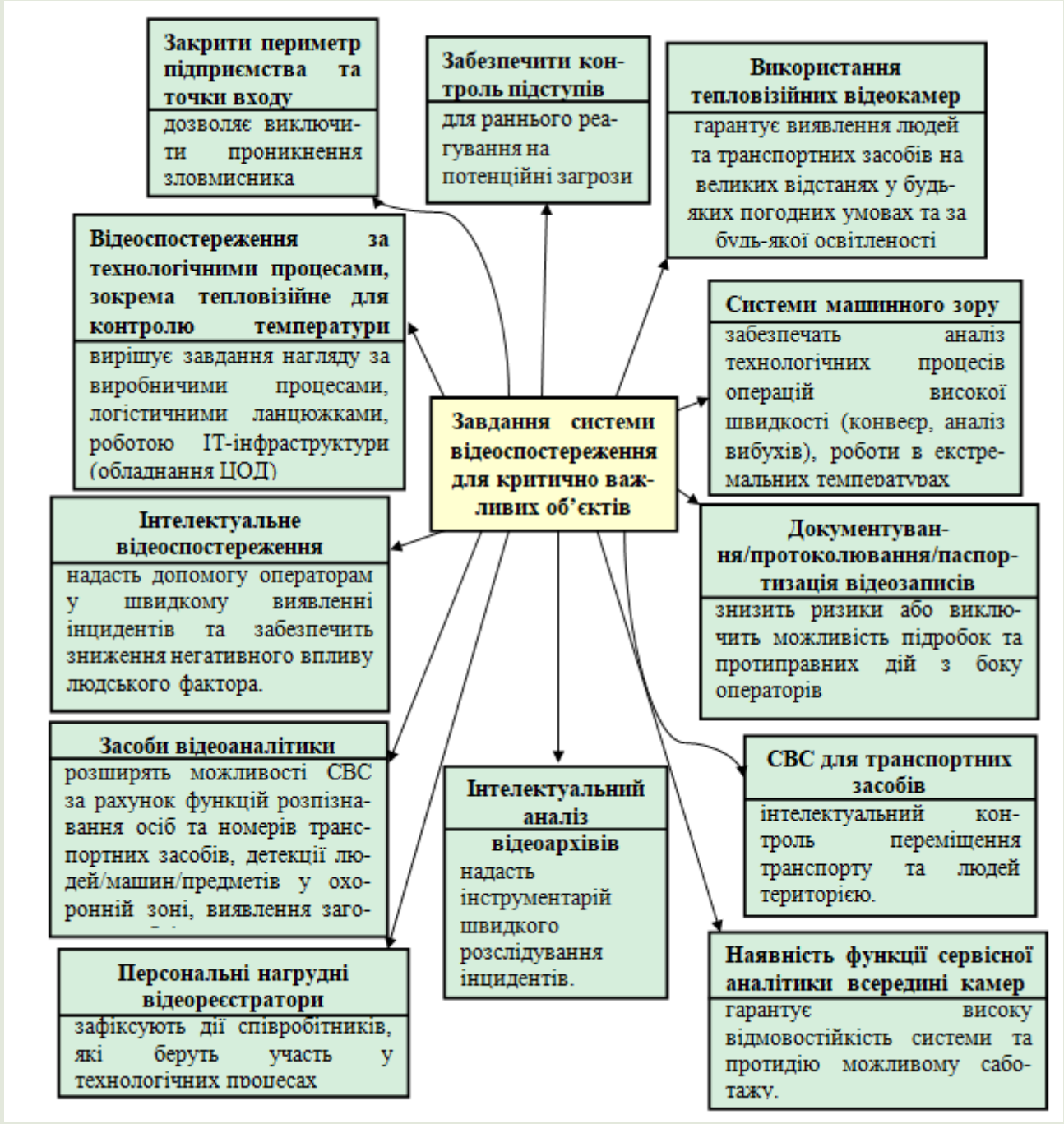
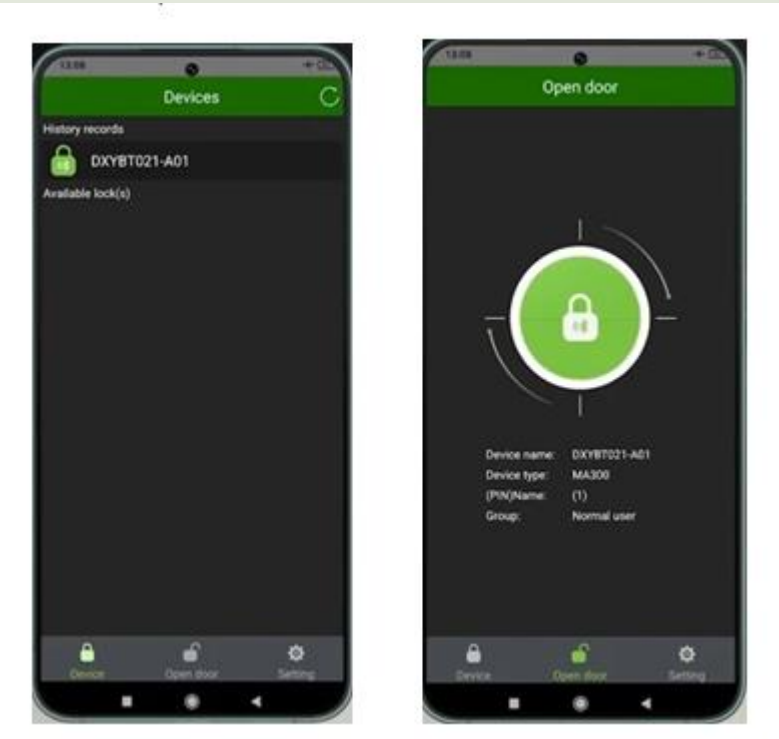
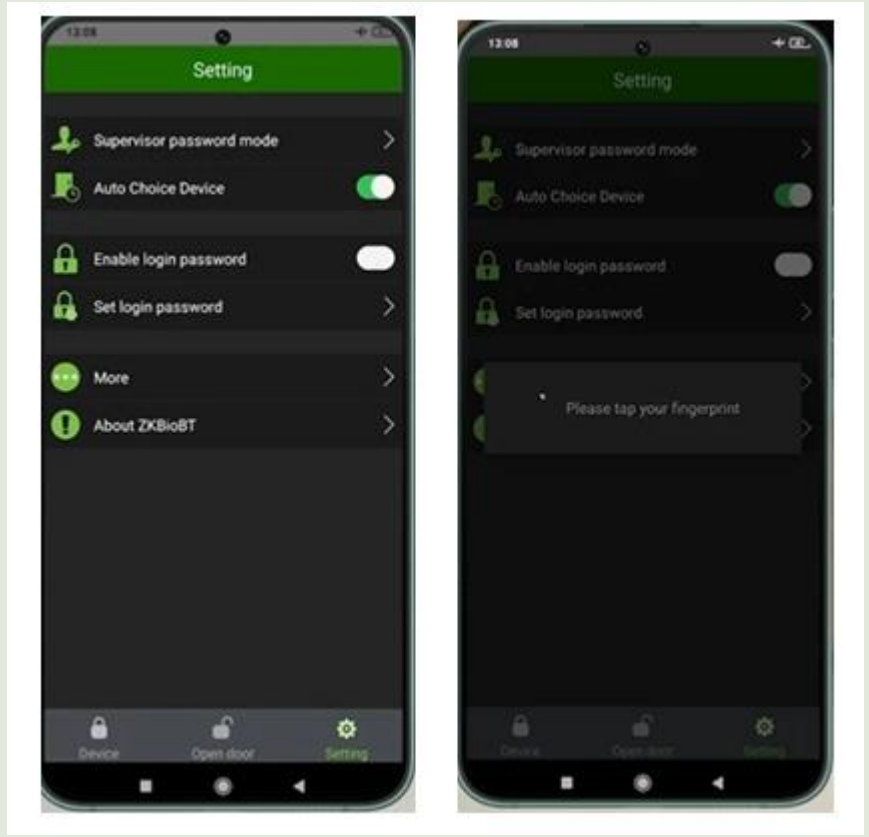



**Схема побудови відеонагляду на критично важливих об'єктах**

# Ідентифікація за відбитком пальця

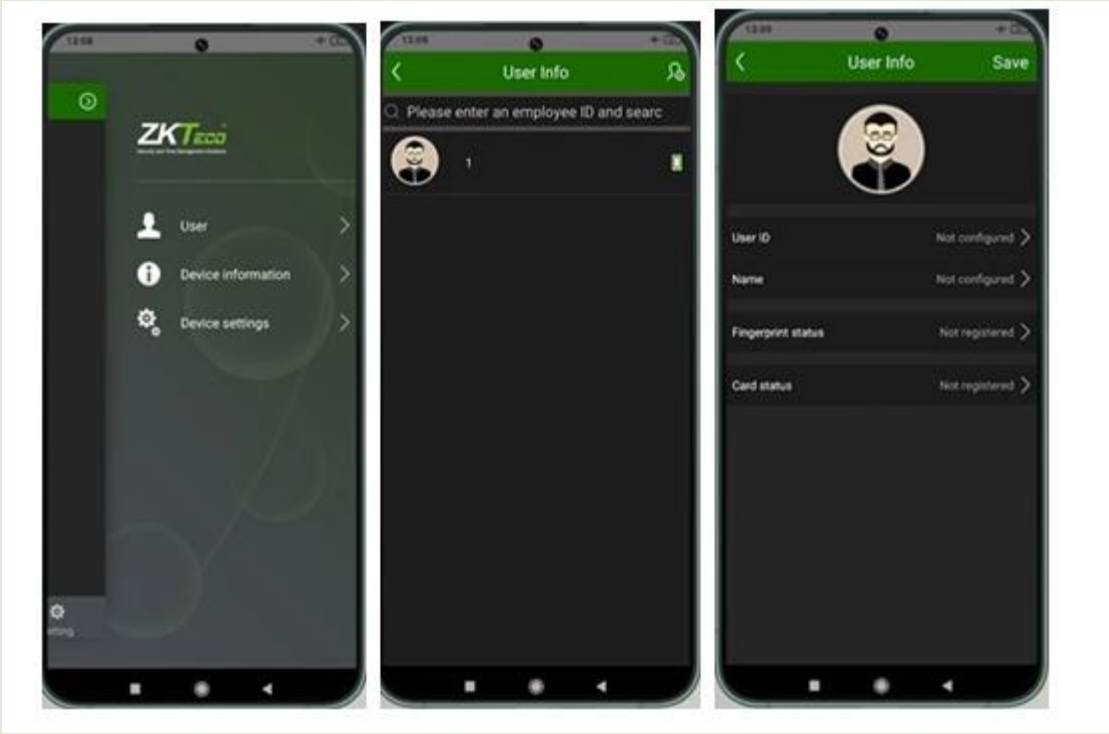


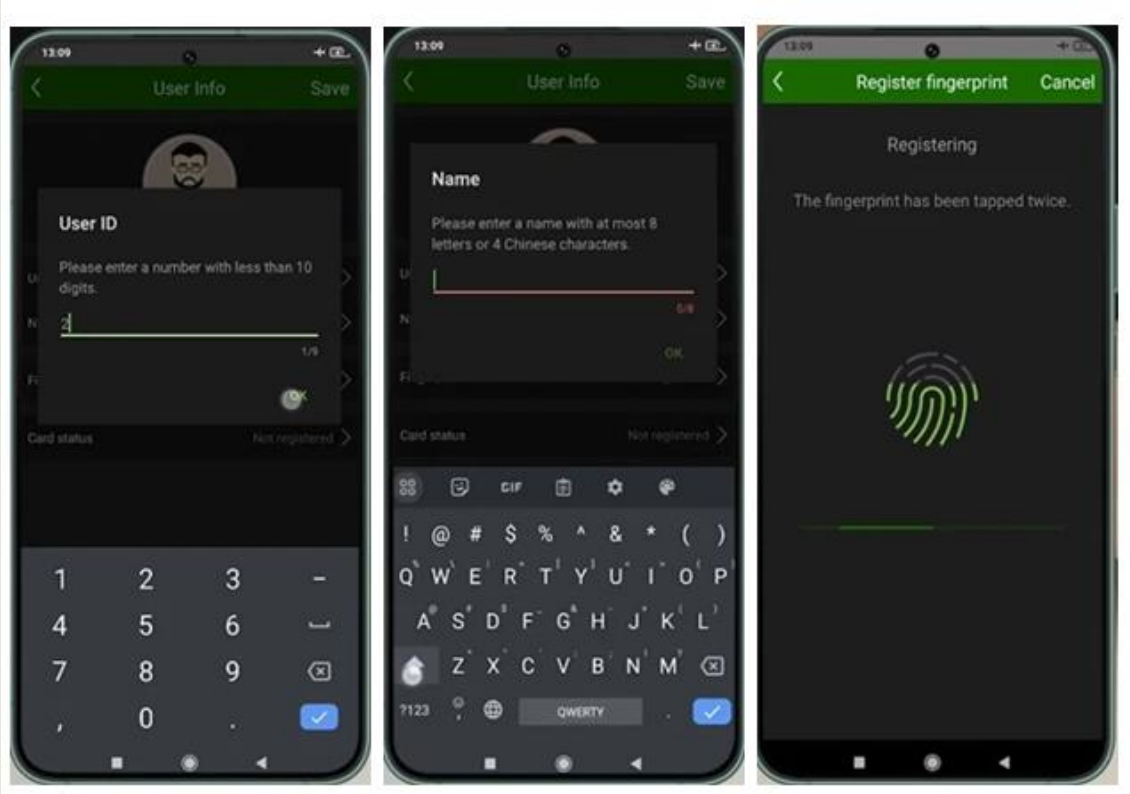

застосунок ZKBioBT



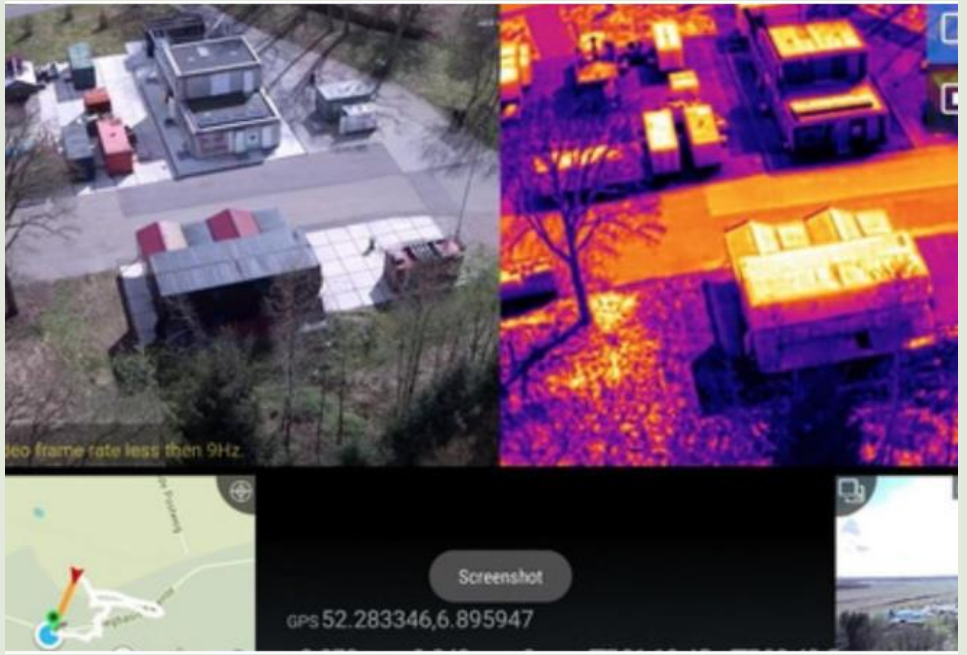

біометричний термінал з Bluetooth ZKTeco MA300-BT/ID

# Ідентифікація за відбитком пальця



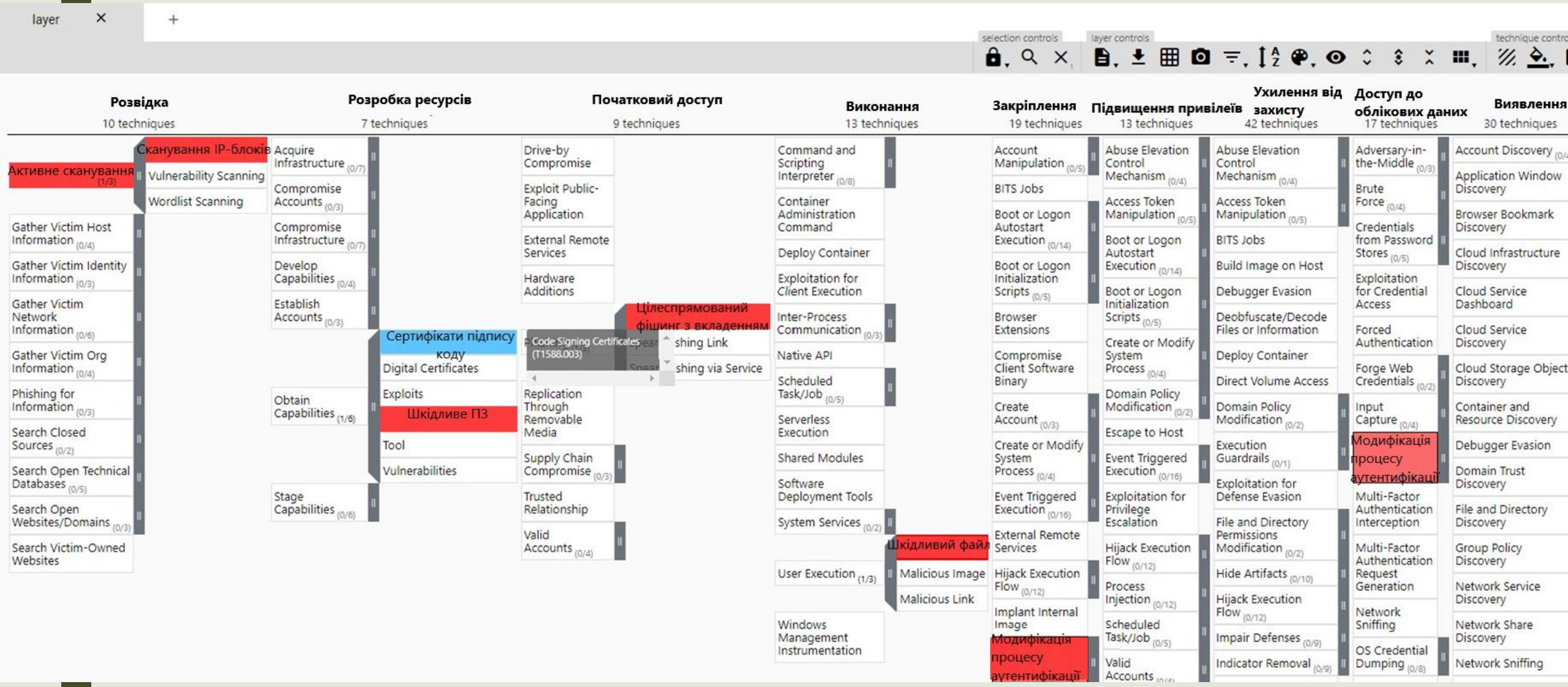



# Використання дронів для охорони периметра критично важливого об’єкта

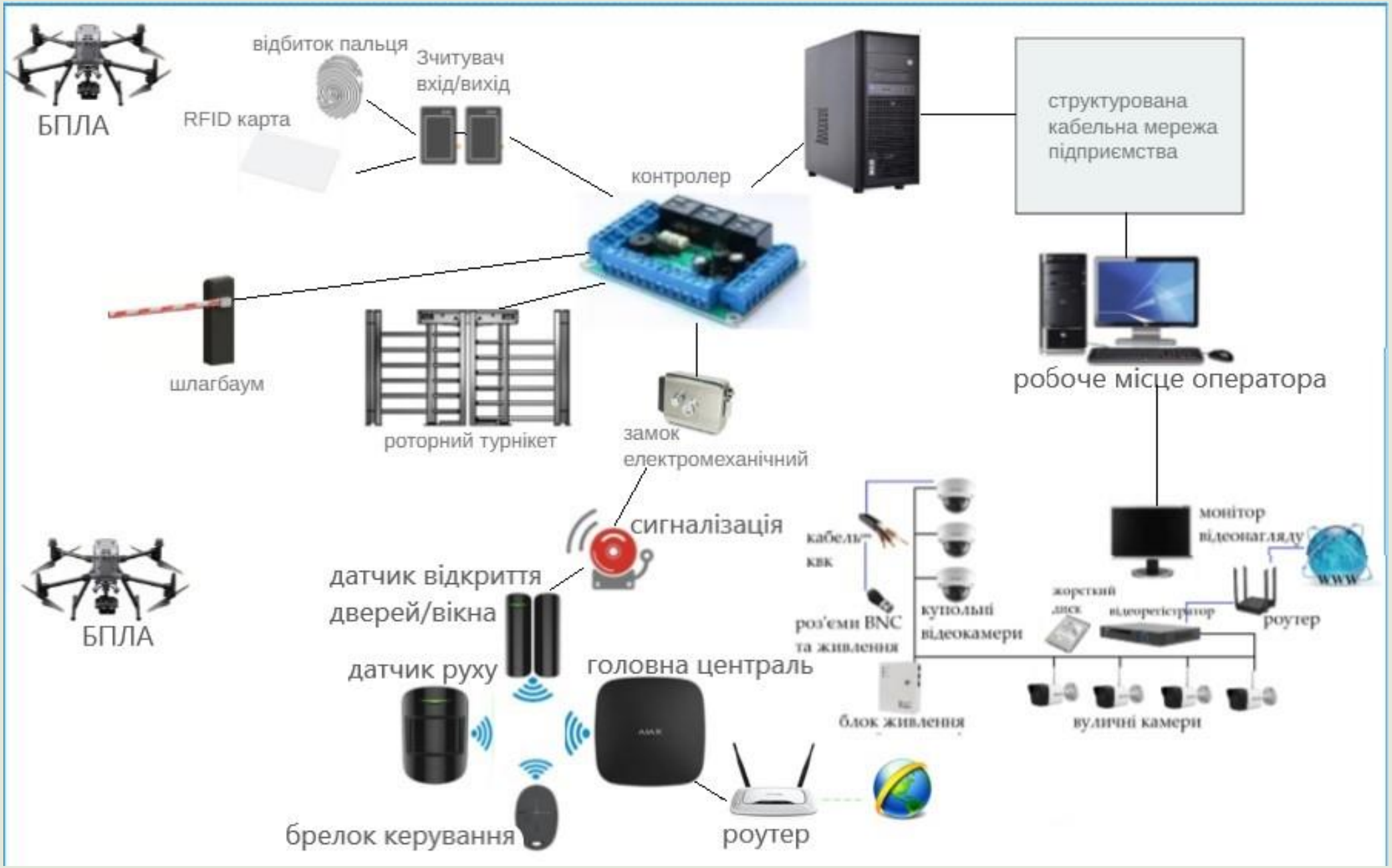



Квадрокоптер дрон DJI Matrice 350 RTK Enterprise + DJI Zenmuse H20T

# Застосування фреймворку Mitre ATT&CK. Процес моделювання векторів атак на компанію.



# Технологія інтелектуального захисту критично важливих об’єктів



# Висновки

-Проведено класифікацію критично важливих об’єктів (КВО)
- Визначені потенційні впливи на КВО.
-Розроблена схема архітектури системи інтелектуального захисту КВО.
-Представлена архітектура системи штучного інтелекту для захисту КВО.
- Описаний алгоритм K-means та Random Forest для класифікації загроз.
-Запропоновано застосування IOT в системах інтелектуального захисту КВО.
-Розроблені моделі атак та визначені методи моніторингу загроз.
-Розроблений алгоритм реагування на інциденти загроз на критичну інфраструктуру.
-Здійснено вибір технічних засобів (система відеоспостереження, система керування доступом, сигналізація та оповіщення, протипожежна система), фізичних засобів захисту КВО – застосування БПЛА для охорони периметру об’єкта,
-Вибір фреймворків та механізмів для захисту КВО (MITRE ATT&CK) та розроблена сама технологія інтелектуального захисту КВО.

**Дякую за увагу!**